CLAIMS

Sub B1

1. A method for performing electronic transactions, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner, and in which an associated public key is kept generally available, characterised in that in connection with an electronic transaction under the sender's own control, preferably through his own input of message information, the sender creates a transaction message, which contains information necessary for the transaction, and, in his smart card, provides the created transaction message with his digital signature while using his own private key for subsequent output and transmission of the transaction message.

2. A method as claimed in claim 1, characterised in that the transaction message contains information on sender, receiver, amount and preferably a transaction serial number.

a

3. A method as claimed in claim 1 ~~or 2~~, characterised in that the transaction message is created off-line, i.e. not connected to the communications network that is used for the subsequent transmission of the transaction message.

4. A method as claimed in claim 3, characterised in that the transaction message is created off-line.

a

5. A method as claimed in ~~any one of the preceding~~ claim~~s~~ 1, characterised in that the transaction message is created in the smart card.

6. A method as claimed in claim 5, characterised in that the transaction message is created with the aid of software inserted in the smart card in advance and preferably also sender information inserted in the card in advance.

a 7. A method as claimed in claim 5 ~~or 6,~~ characterised in that information required for the transaction message is input with the aid of input means arranged on the smart card, the card preferably being a so-called advanced smart card.

a 8. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-6~~, characterised in that information necessary for the transaction message is input with the aid of a protected card terminal.

a 9. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-6~~, characterised in that information necessary for the transaction message is input with the aid of a separate card communication unit, the latter preferably also being a card activator.

a 10. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-6~~, characterised in that information necessary for the transaction message is input with the aid of a telecommunications unit controlled by the smart card, especially a mobile telecommunications unit such as a mobile phone.

Cont B1

a 11. A method as claimed in ~~any one of the preceding~~ claim~~s~~, 1 characterised in that the transaction message contains sender information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

a 12. A method as claimed in ~~any one of the preceding~~ claim~~s~~, 1 characterised in that the transaction message contains receiver information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

a 13. A method as claimed in ~~any one of the preceding~~ claim~~s~~, 1 characterised in that the signed transaction message is sent to a card or account administrator regarding the sender or receiver, that the digital signature of the transaction message is authenticated by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that in case of authenticity, the receiver is credited with the transaction amount by a clearing process.

14. A method as claimed in claim 13, characterised in that the signed transaction message is first sent to the receiver, who optionally after his own checking of the digital signature of the message forwards the signed transaction message to said card or account administrator.

a

B' Cont

15 A method as claimed in ~~any one of~~ claim~~s~~ 1~~-12~~, characterised in that the signed transaction message is encrypted by using a public key belonging to the addressee, to whom the transaction message is sent, that the encrypted, signed transaction message is sent to the addressee, that the addressee by using his private key decrypts the signed transaction message, that the digital signature of the transaction message is authenticated by using the public key which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

16. A method as claimed in claim 15, characterised in that the addressee is the receiver, that the receiver, after decryption, sends the signed transaction message to a card or account administrator, whereupon said authentication takes place.

a

17. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-12~~, characterised in that the signed transaction message is encrypted by using the sender's public key and is provided with sender information and is then sent to a card or account administrator, who has the sender's private key and who preferably has issued the user's smart

card, that said administrator decrypts the received encrypted message by using said private key, that authentication of the digital signature of the decrypted transaction message takes place by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

a

18. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-14~~, characterised in that the signed transaction message is sent non-encrypted, especially via a public communications network, such as the Internet or a telecommunications network.

a Cont'

19. A method as claimed in ~~any one of the preceding~~ claim~~s~~, 1 characterised in that the signed transaction message is sent by e-mail.

a B'

20. A method as claimed in ~~any one of~~ claim~~s~~ 1~~-18~~, characterised in that the signed transaction message is sent via a mobile telephone network, especially by using a so-called SMS service.

21. A smart card for carrying out electronic transactions, comprising means for storing card identification information, means for protected storing of a private key, means for storing an asymmetrical algorithm, means for input of transaction information into the card, processor means for creating in the card a transaction message based on input transaction information, such as information on amount and receiver, and optionally information stored in the card, such as information on sender and preferably a serial number, and for providing the transaction message with a digital signature on the basis of said private key and said asymmetrical algorithm, and means for output of the signed transaction message.

22. A card as claimed in claim 21, characterised in that it is of a so-called advanced type.

23. A combination of a smart card and a user-controlled communication unit, which is arranged for commu-

nication with the smart card and with which the card is adapted to be combined with a view to producing an electronic transaction message, the card comprising means for protected storing of a private key, means for storing an asymmetrical algorithm and processor means for providing a created transaction message with a digital signature based on said private key and said algorithm, and said communication unit comprising means for input of transaction information, and means being arranged in the communication unit and/or in the card for creating said transaction message.

Cont B1

24. A combination as claimed in claim 23, characterised in that the communication unit is a mobile telecommunication device.

25. A combination as claimed in claim 23, characterised in that the communication unit is a combined card activator and information inputter/processor.

26. Use of a smart card with a private key stored therein for providing, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

add a1 >